CLAIMS

What is claimed is:

1. A firewall capable of creating a plurality of trust levels for a plurality of computer networks.
2. The firewall of claim 1 comprising:

   a plurality of rules; and

   a table defining the relationship between the trust levels, the rules, and the computer networks.
3. The firewall of claim 2, wherein the firewall further comprises: a configuration program, wherein the configuration program allows a user to add, delete, or modify the rules and trust levels in the table.
4. The firewall of claim 2, wherein the firewall further comprises: a security program, wherein the security program analyzes a packet and determines if the rules permit or deny the packet.
5. The firewall of claim 4, wherein the security program comprises:

   instructions for determining the destination of the packet;

   instructions for determining the appropriate rules to use to analyze the packet using the table;

   instructions for analyzing the packet using the rules;

   instructions for determining if the packet is permitted under the rules;

   responsive to a determination that the rules permit the packet, instructions for permitting the packet; and

   responsive to a determination that the rules deny the packet, instructions for denying the packet.

6. The firewall of claim 5, wherein the security program further comprises: responsive to a determination that the rules do not permit or deny the packet, instructions for denying the packet.
7. The firewall of claim 1 wherein the firewall is part of a router.

8. A router comprising:

a switch connected to a firewall and a plurality of computer networks; and

wherein the firewall creates a plurality of trust levels and associates a trust level with each computer network.

9. The router of claim 8 wherein the switch comprises a sub-switch, the sub-switch being assigned one of a plurality of trust levels.
10. The router of claim 8 wherein the firewall analyzes a packet using some of the rules; and wherein the rules used in the lower trust levels are excluded from the rules used to analyze the packet.
11. The router of claim 8, wherein the firewall further comprises: a configuration program, wherein the configuration program allows a user to add, delete, or modify the rules and trust levels in the table.
12. The router of claim 8, wherein the firewall further comprises: a security program, wherein the security program analyzes a packet and determines if the rules permit or deny the packet.
13. The router of claim 12, wherein the security program comprises:

instructions for determining the sub-switch location of the packet;

instructions for determining a source of the packet;

instructions for determining a destination of the packet; and

instructions for determining if the packet is attempting to go to a higher trust level;

responsive to a determination that the packet is not attempting to go to a higher trust level, instructions for permitting the packet.

14. The router of claim 13, wherein responsive to a determination that the packet is attempting to go to a higher trust level, the security program further comprises:

instructions for determining the appropriate rules to use to analyze the packet using the table;

instructions for analyzing the packet using the rules;

instructions for determining if the packet is permitted under the rules;

responsive to a determination that the rules permit the packet, instructions for permitting the packet; and

responsive to a determination that the rules deny the packet, instructions for denying the packet.

15. The router of claim 14, wherein the security program further comprises: responsive to a determination that the rules do not permit or deny the packet, instructions for denying the packet.

16. The router of claim 8 wherein the firewall further comprises: a table defining the relationship between the trust levels, the rules, and the computer networks.

17. A method for analyzing a packet using a firewall which creates a plurality of trust levels for a plurality of computer networks, the method comprising:

determining the destination of the packet;

accessing a plurality of rules;

determining the appropriate rules to use to analyze the packet;

analyzing the packet using the rules;

determining if the packet is permitted under the rules;

responsive to a determination that the rules permit the packet, permitting the packet; and

responsive to a determination that the rules deny the packet, denying the packet.

18. The method of claim 17 further comprising: responsive to a determination that the rules do not permit or deny the packet, denying the packet.

19. The method of claim 17 wherein a table defines the relationship between the trust levels, the rules, and the computer networks.

20. A method for analyzing a packet using a firewall which creates a plurality of trust levels for a plurality of computer networks, the method comprising:

determining the sub-switch location of a packet;

determining a source of the packet;

determining a destination of the packet;

determining if the packet is attempting to go to a higher trust level; and

responsive to a determination that the packet is not attempting to go to a higher trust level, permitting the packet.

21. The method of claim 20, wherein responsive to a determination that the packet is attempting to go to a higher trust level, the method further comprises:

determining the appropriate rules to use to analyze the packet using the table;

analyzing the packet using the rules;

determining if the packet is permitted under the rules;

responsive to a determination that the rules permit the packet, permitting the packet; and

responsive to a determination that the rules deny the packet, denying the packet.

22. The method of claim 21 wherein the security program further comprises: responsive to a determination that the rules do not permit or deny the packet, denying the packet.

23. The method of claim 20 wherein the firewall further comprises: a table defining the relationship between the trust levels, the rules, and the computer networks.

24. A program product operable on a computer, the program product comprising:

a computer-usable medium;

wherein the computer usable medium comprises instructions comprising:

instructions for determining the destination of the packet;

instructions for accessing a plurality of rules;

instructions for determining the appropriate rules to use to analyze the packet;

instructions for analyzing the packet using the rules;

instructions for determining if the packet is permitted under the rules;

responsive to a determination that the rules permit the packet, instructions for permitting the packet; and

responsive to a determination that the rules deny the packet, instructions for denying the packet.

25. The program product of claim 24 further comprising: responsive to a determination that the rules do not permit or deny the packet, instructions for denying the packet.

26. The program product of claim 24 wherein a table defines the relationship between the trust levels, the rules, and the computer networks.

27. A program product operable on a computer, the program product comprising:

a computer-usable medium;

wherein the computer usable medium comprises instructions comprising:

instructions for determining the sub-switch location of a packet;

instructions for determining a source of the packet;

instructions for determining a destination of the packet;

instructions for determining if the packet is attempting to go to a higher trust level; and

responsive to a determination that the packet is not attempting to go to a higher trust level, instructions for permitting the packet.

28. The program product of claim 27, wherein responsive to a determination that the packet is attempting to go to a higher trust level, the method further comprises:

instructions for determining the appropriate rules to use to analyze the packet using the table;

instructions for analyzing the packet using the rules;

instructions for determining if the packet is permitted under the rules;

responsive to a determination that the rules permit the packet, instructions for permitting the packet; and

responsive to a determination that the rules deny the packet, instructions for denying the packet.

29. The program product of claim 28 wherein the security program further comprises: responsive to a determination that the rules do not permit or deny the packet, instructions for denying the packet.

30. The program product of claim 27 wherein the firewall further comprises: a table defining the relationship between the trust levels, the rules, and the computer networks.

31. A firewall capable of creating a plurality of trust levels for a plurality of computer networks comprising:

a plurality of rules;

a table defining the relationship between the trust levels, the rules, and the computer networks;

a configuration program, wherein the configuration program allows a user to add, delete, or modify the rules and trust levels in the table;

a security program, wherein the security program analyzes a packet and determines if the rules permit or deny the packet, the security program comprising:

instructions for determining the destination of the packet;

instructions for determining the appropriate rules to use to analyze the packet using the table;

instructions for analyzing the packet using the rules;

instructions for determining if the packet is permitted under the rules;

responsive to a determination that the rules permit the packet, instructions for permitting the packet;

responsive to a determination that the rules deny the packet, instructions for denying the packet; and

responsive to a determination that the rules do not permit or deny the packet, instructions for denying the packet.

32. The firewall of claim 31 wherein the firewall is part of a router.